「ICTサイバーセキュリティ総合対策2021（案）」
に対する意見

2021年7月8日

BSA｜ザ・ソフトウェア・アライアンス[1]（以下、「BSA」）は、総務省（以下、「貴省」）の「ICT サイバーセキュリティ総合対策 2021（案）」（以下、「対策案」）に対して、以下のコメントを提出する機会を与えられたことに感謝します。

総論

BSA は、政府やグローバル市場において、世界のソフトウェア産業を代表する主唱者です。BSA の会員は、クラウドコンピューティング、モノのインターネット（IoT）、人工知能（AI）、また、その他の新たなイノベーションをもたらす製品やサービスなど、世界経済の成長を促進するソフトウェアを活用した技術革新の最前線にいます。また、BSA の会員は、現在、業界全体で使用されているソフトウェア・セキュリティのベスト・プラクティスの多くを開拓した、セキュリティのリーダーでもあります。

BSA は、昨年、「IoT・5G セキュリティ総合対策 2020（案）」に対して意見書[2]を提出しており、貴省が引き続き、日本のデジタル・トランスフォーメーションを推進し、国民が様々なデジタルサービスを安全に利用できる環境を整備することに重点を置き、サイバーセキュリティの向上に向けて取り組まれていることを高く評価しています。また、IoT、5G、クラウドベースのサービスなどの技術を安全に導入・利用するためのハイレベルなガイドラインの策定や、テレワークの重要性を認識されていること、国際的なサイバーセキュリティ・コミュニティと緊密に連携してクラウドベースの技術活用に取り組まれていることを支持します。

[1] BSA の活動には、Adobe, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, Workday, Zoomが会員企業として参加しています。詳しくはウェブサイト（http://bsa.or.jp）をご覧ください。

[2] https://bsa.or.jp/wp-content/uploads/20200626j.pdf

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org
Japan Representative Office

「自由、公正、かつ安全なサイバー空間」の実現に向けて、ICT に係るインフラやサービスのサイバーセキュリティを確保するという貴省の目標を支援するため、以下、意見を述べさせて頂きます。

提言

II. 情報通信サービス・ネットワークの個別分野に関する具体的な対策 /3 (2) クラウドサービスの利用の進展を踏まえた対応

対策案に記載されているように、エンドユーザによる障害や設定ミスが発生しているものの、これらはオンプレミスや他の類似したサービスと重大な違いは無く、現在のクラウドで利用可能なセキュリティツールは、責任共有モデルと合わせ、最高レベルのセキュリティ実践を確保する包括的なものとなっています。

対策案の中で的確に認識されているように、クラウドコンピューティングは、コスト削減、情報システムの迅速な整備、柔軟なリソースの増減、自動化された運用による高度な信頼性、災害対策、テレワーク環境の実現、といった多大な恩恵をもたらします。また、クラウドコンピューティングは、サイバーセキュリティの面でも大きく寄与します。日本がデジタルト・ランスフォーメーションを実現し、これらのメリットを十分に活用するためには、政府においてクラウドコンピューティング・サービスが広く導入されることが不可欠であり、対策案で示されているように、このために、政府機関が調達するクラウドサービスのセキュリティを評価する「政府情報システムのためのセキュリティ評価制度」（ISMAP）が昨年開始されました。 クラウドサービスプロバイダー（CSP）に対する基本的なセキュリティ要件を設定した、本制度の発足を支持する一方、公共部門における「クラウド・バイ・デフォルト原則」の実現という日本政府の目標を促進し、また、本格的なデジタル・トランスフォーメーションを可能にするサイバーセキュリティへの取り組みを支える上で、ISMAP の実施があまりにも煩雑で高額な費用を要していることに、我々は懸念を抱いています。

ISMAP には 1,000 以上の管理項目が掲載されているため、サービスを提供する企業や ISMAP 認証の取得を希望する企業には大きなコンプライアンス負担と法外なコストが課せられ、多くの CSP にとって ISMAP 認証の魅力が低下します。その結果、ISMAP クラウドサービスリストに登録され、日本の公共機関にサービスを提供できる CSP の数が不必要に制限される可能性があります。

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org
Japan Representative Office

我々は、以下の点を考慮に入れ、政府が継続的に ISMAP の改善を検討することを奨めます。

・様々なクラウドサービスのモデル（SaaS、IasS、PaaS）の特徴的な要件を考慮して、 これらのサービスのリスクを管理するために最適化された必須のセキュリティ管理を定義することにより、現行の ISMAP をより柔軟で、実施しやすくすること。

・ISMAP を適用するにあたっては、中核となる基本的な管理策を対象とし、その他の追加の管理策については、実施される特定の状況下における必要に応じて適用されるようにし、広く採用されている国際規格、および調達側との間で締結された契約における追加要件に基づくこと。

・国際的なクラウド・セキュリティのベスト・プラクティスに沿った、頻度を減らした監査スケジュール（例：三年に一度）を設定し、CSP と政府双方の監査作業を削減すること。毎年の監査では、CSP は連続して監査プロセスを実施しな くてはならず、常時、監査対応に追われることとなり、セキュリティ担当者の注意を不必要にそらすこととなります。調達省庁側にとっても、年度の契約更新の負荷が増すこととなります。

・申請・登録の受付を、四半期ごとではなく、年間を通じて行うことができるようにすること。年に 4 回の申請・登録に限定されると、CSP にとっては、3 ヶ月以上の遅れが生じる可能性があります。年間を通して継続的に申請・登録を行うことで、ISMAP は急速に進化するクラウドの技術に対応することが可能となります。

・ISMAP の開発プロセスと並行して、日本におけるクラウドサービスのための IT 監査・ 認証要員の訓練・育成をするための手続を開発し、適切な人材を確保すること。

・クラウドサービスの責任共有モデル[3]を強調し、周知徹底させること。対策案において、責任共有モデルが認識されていることを我々は高く評価しており、政府機関全体において本モデルが理解されるよう、貴省が先導をとることを奨励します。ISMAP に責任共有の原則を明確に盛り込むことで、クラウドサービスのリスク管理をするための管理基準の設定と維持において、CSP と顧客との間とのクラウド運用に関する異なる責任が適切に認識されるようになります。また、自らが管理し、責任を負う環境の側面において、どの当事者が説明責任を負うのかを明確にすることができます。これにより、アクセス権を持たない顧客データやシステムに対して、CSP にセキュリティ要件や義務を課すという、セキュリティやプライバシーにとって逆効果をもたらすような状況を避けることができます。クラウド導入を成功させるには、クラウド利用者や調達者が、クラウド環境で安全なアプリケーションを開発し、必要に応じてサービ

[3] https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/

ス・ プロバイダーが提供するツールや対策を自らの責任で利用し、セキュリティ・リスク を最小限に抑えることが求められている、ということが理解されることが重要です。

・ 第三者による、国際的な認証および監査結果を、ISMAP の関連する管理基準および要件に準拠している証跡として認めること。これにより、実用的でない、現地監査の必要性が減ります。現地監査は、本目的以外では権限を持たない者による現場へのアクセスを要するため、データセンターを不必要な物理的セキュリティ・リスクにさらすことになります。

また、日本のデジタル・トランスフォーメーション（DX）という目標を支えるために、革新的で順応なセキュリティ・アプローチを可能にするようなクラウド・セキュリティ政策を採用することを強く推奨します。これにより、セキュリティへのリスク対応や回復力といった、クラウド技術が可能とする利点を効果的に活用することが可能となります。

この観点から、ISMAP の見直しに加え、「地方公共団体における情報セキュリティポリシーに関するガイドライン」[4]において、地方公共団体に対して、マイナンバー・データを管理する情報システムの物理的なネットワーク分離の実施を推奨するような、時代にそぐわないセキュリティアプローチを排除することを求めます。国民のプライバシーや個人情報を保護する意図を我々は十分に理解し、支持しますが、このような政策は、導入のための高額な費用を発生させ、当該データの想定通りの利用を可能にする、革新的なクラウドベースの技術やサービスを活用する上で大きな障害となります。また、ネットワーク分離は、逆にシステムの安全性を低下させる可能性があります。

独立したネットワーク構築のためには、独立したサーバー、ルーター、スイッチ、管理ツールなど、ネットワークをサポートするために必要なインフラを構築する費用が必要となり、生産性や効率性が低下します。接続されたネットワークと分離されたネットワークやデバイスの間で情報を管理することは、時間を要するだけでなく、混乱やエラーも引き起こし、さらなるセキュリティリスクにつながる可能性があります。

多くのクラウドサービスは、暗号化や厳格なアクセス管理システムなど、国際的に認められた機能を実装することで、世界水準のデータセキュリティを実現しています。[5]BSA 会員を含む多くのグローバルな CSP は、データ・セキュリティへの大規模な投資をしており、利用可能な機微個人情報のために、最も効果的なデータ・セキュリティを提供しています。これらの最高水準の安全なソリューションの使用を可能にすることを、日本政府が政策によって確かなものとすることが不可欠であると、我々は考えます。これらの最高水準のデータ・セキュリティ・ソリューションは、リスクベースで成果重視の手法を採用しています。採用されているのは、ゼ

[4] https://www.soumu.go.jp/main_content/000726079.pdf

[5] BSA International Cybersecurity Policy Framework
https://bsacybersecurity.bsa.org/report-item/bsa-international-cybersecurity-policy-framework

ロトラスト・セキュリティ・アーキテクチャー[6]、高度なユーザーID 管理とアクセス制限システム、常時接続の仮想プライベート・ネットワークや仮想ネットワーク・セグメンテーションなどのネットワーク制御、ネットワーク層に加えてデータ・ベース層での強力なデータ暗号化など、「多層防御」[7]に基づいたセキュリティ・アプローチです。

また、ゼロトラスト・セキュリティ・アーキテクチャの考え方は、「暗黙の信頼ゾーン（implicit trust zone）」を可能な限り最小化することであるため、データを暗号化してオペレーターからも見えないようにしたり、システムの設計・開発段階で操作ミスをなくす努力をするなど、考え方に沿った様々なセキュリティ対策を行う必要があります。これらの対策は、一見するとサイバーセキュリティに直接関連してないように思えるかもしれませんが、ネットワークのセキュリティを含めた IT システム全体のセキュリティを確保する上で、非常に有効なアプローチとなります。

以上のことから、時代にそぐわない物理的なネットワーク分離やデータローカライゼーション要件を改め、現在の技術に合わせたセキュリティソリューションを採用し、成果重視のリスク管理制御に焦点を当て、「多層防御」の原則に基づいたベストプラクティスを採用し、安全なクラウドコンピューティングサービスの調達と利用を通じて政府業務をより効果的に推進させることを貴省に求めます。

サイバーセキュリティのソリューションは、官民が連携し、市場主導型のソリューションを採用する時に最も効果を発揮します。[8] BSA と BSA 会員企業は、ISMAP の改善、また、意識向上のための教育プログラム提供など、貴省と協力し、官民双方で「クラウド・バイ・デフォルト原則」を推進していきたいと考えています。

III 横断的施策／ １ サイバーセキュリティ情報に関する産学官での連携・共有等の促進

デジタル改革・DX 推進の前提として安全なサイバー環境を構築するためには、産学官連携によるサイバー攻撃等に関する情報の収集・分析を促進することが有用であるとする、貴省の見解を、我々は全面的に支持します。自主的なデータ共有の取り決めを促進することは、社会全体のセキュリティ対策のレベルを高めることに貢献します。また、サイバーセキュリティの脅威は性質上、グローバルであり、国境に隔てられているわけではありません。効果的な分析と調査のためには、サイバー攻撃に有効な脅威情報が広く可視化されていなくてはなりません。

---

[6] Zero Trust Architecture, NIST SP-800-207
https://www.nist.gov/publications/zero-trust-architecture

[7] NISTでは「多層防御（Defense-in-Depth）」は「人、技術、および業務遂行能力を統合して、組織内の階層およ びミッションごとに複数の調節可能な防壁を築く情報セキュリテ ィ戦略」と定義されています。
https://www.ipa.go.jp/files/000056415.pdf
https://csrc.nist.gov/glossary/term/defense_in_depth

[8] https://bsacybersecurity.bsa.org/report-item/bsa-international-cybersecurity-policy-framework

可視化は、様々な情報源から可能となります。対策案に記載されている、ISAC のような特定分野ごとの情報共有や分析センターのような選択肢に加え、顧客のインストール先、発表されている脆弱性、脅威を共有するネットワーク等から得ることも可能です。意義ある分析のために脅威情報を集めることは、脅威の調査が実施される場所には関係しません。また、サイバーセキュリティの強化は、導入されている技術が国内か海外のものかによって左右されるものではありません。

日本国内のベンダーは、海外の事業者同様、日本の情報源だけでなく、世界中の情報源から脅威情報を得て、研究することができます。国内と海外ベンダー間の脅威情報共有の取り決めは、有効な脅威データを集め、国内の能力開発を可能とし、対策案に記されている「データ負けのスパイラル」を防ぐことができます。BSA 会員企業の多くは、そのような情報共有の取り決めを促進しています。貴省が情報共有を強化し、エンジニアをグローバルな規模で育成し、また、生産国に関係なく利用可能な最良のセキュリティ技術を確実に採用することに注力することを奨めます。これにより、日本特有のサイバーセキュリティ・モデルが世界と相容れなくなり、日本が国際的にサイバーセキュリティでリーダーシップを発揮できなくなる事態を回避することができます。

結語

上記意見が、「対策案」を最終的に確定する上で有効であれば幸いです。データ・フリー・フロー・ウィズ・トラスト（DFFT）を推進するために、貴省がサイバーセキュリティに関し、国際的なリーダーシップを発揮することを我々は支援します。また、日本のデジタルトランスフォーメーションを推進するために、貴省と協力してサイバーセキュリティを強化していくことを期待しています。本意見に関して、ご質問がある場合又はより詳細に議論をされたい場合には是非ご連絡下さい。